WHAT IS CLAIMED IS:

1. A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and one or more network infrastructures, the method comprising the steps of:

a. monitoring the network system for intrusions;

b. upon detection of an intrusion, identifying one or more sources of the intrusion;

c. identifying one or more enforcement devices of the network system associated with the one or more identified sources; and

d. configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion.

2. The method as claimed in Claim 1 wherein the step of identifying the one or more sources of the intrusions includes the step of identifying a physical address and/or a logical address of each of the one or more identified sources.

3. The method as claimed in Claim 2 wherein the physical address information is a MAC address and/or the logical address information is an IP address.

4. The method as claimed in Claim 1 wherein the step of monitoring the network for intrusions is performed by an intrusion detection function.

5. The method as claimed in Claim 4 wherein the intrusion detection function is a centralized function.

6. The method as claimed in Claim 4 wherein the intrusion detection function is a distributed function.

7. The method as claimed in Claim 4 wherein the intrusion detection function is an intrusion detection system.

8. The method as claimed in Claim 1 wherein the step of identifying the one or more enforcement devices associated with the one or more identified sources includes the step of determining the physical address, logical address, or both for each of the identified one or more enforcement devices.

9. The method as claimed in Claim 1 further comprising the step of verifying the identification of the identified one or more sources.

10. The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the identified one or more enforcement devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by the identified one or more sources, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the identified one or more enforcement devices, to or from one or more other network infrastructure devices, or to or from any of the attached functions not identified as an intrusion source, and directing all signals exchanged by the identified one or more sources to a honeypot, a second intrusion detection function, a monitoring device, or a simulation device.

11. The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the identified one or more enforcement devices to permit connectivity of the identified one or more sources while dampening the level of activity associated with the identified one or more sources to minimize network harm while permitting analysis and auditing of the identified one or more sources and the gathering of forensic evidence.

12. The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes includes the steps of first configuring a first set of one or more enforcement devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more

intrusions related to the intrusions causing the first one or more policy changes, configuring a second set of one or more enforcement devices with a second set of one or more policy changes.

13. The method as claimed in Claim 12 wherein one or more of the one or more enforcement devices of the second set are enforcement devices of the first set.

14. The method as claimed in Claim 1 wherein the identified one or more enforcement devices are selected from the group consisting of network entry devices and centralized switching devices.

15. The method as claimed in Claim 1 wherein the one or more policy changes are configured on one or more ports of one or more of the identified one or more enforcement devices.

16. A Distributed Intrusion Response System (DIRS) to respond to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and a network infrastructure, the DIRS comprising:

a. a directory service function for receiving address information for attached functions and devices of the network infrastructure;
b. a policy manager function for configuring devices of the network infrastructure with policies;
c. means for identifying one or more sources of one or more intrusions; and
d. one or more enforcement devices of the network infrastructure, wherein each enforcement device is configured to enforce policy changes established thereon by the policy manager function in response to one or more detected intrusions.

17. The DIRS as claimed in Claim 16 further comprising a policy decision function configured:

a. to receive detected intrusion information from an intrusion detection function;
b. to receive network infrastructure device information from the directory service function;

c. to evaluate whether a policy change or changes is or are required on one or more of the security enforcement devices in response to the detected intrusion information; and

d. to direct the policy manager function to configure one or more identified enforcement devices with determined policy changes upon deciding to do so based upon the evaluation.

18. The DIRS as claimed in Claim 17 wherein the policy manager function and the policy decision function are part of a central server of the network infrastructure.

19. The DIRS as claimed in Claim 18 wherein the directory service function is part of the central server.

20. The DIRS as claimed in Claim 17 wherein the intrusion detection function is provided by an intrusion detection system of the network infrastructure.

21. The DIRS as claimed in Claim 17 wherein the intrusion detection function is a distributed intrusion detection function.

22. The DIRS as claimed in Claim 17 wherein the intrusion detection function is a centralized intrusion detection function.

23. The DIRS as claimed in Claim 16 wherein the one or more network security enforcement devices is selected from the group consisting of routers, switches, access points, gateways, and firewalls.

24. The DIRS as claimed in Claim 16 further comprising a network management system for identifying address information for the network security enforcement devices.

25. The DIRS as claimed in Claim 24 wherein the network management system communicates with the intrusion detection function.

26. The DIRS as claimed in Claim 16 wherein the directory service function is distributed among a plurality of devices of the network infrastructure.

27. The DIRS as claimed in Claim 16 further comprising means to validate the accuracy of the identity of the identified one or more sources including a logical address, a physical address, or a location.